



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/708,838	03/26/2004	Blayn W. Becnau	70655.0200	2837
20322	7590	04/18/2006	EXAMINER	
SNELL & WILMER ONE ARIZONA CENTER 400 EAST VAN BUREN PHOENIX, AZ 850040001			WALSH, DANIEL I	
			ART UNIT	PAPER NUMBER
			2876	

DATE MAILED: 04/18/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/708,838

Applicant(s)

BEENAU ET AL.

Examiner

Daniel I. Walsh

Art Unit

2876

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 21 February 2006.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,2,4-13 and 15-21 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,2,4-13 and 15-21 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. Receipt is acknowledged of the RCE received on 21 February 2006.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claim 20 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The Examiner notes that claim 20 recites that first and second user information are associated with different users. However, the specification teaches that the sample is of the same user and that it is primarily and secondarily associated with accounts (such as for overdraft protection or for switching accounts when one account is low or has inadequate funds). The specification does not teach that the samples are from different users, but in fact, from the same user.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 20 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Re claim 20, it is unclear how one sample can be associated with two different users.

Appropriate clarification/correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

4. Claims 1-2, 4-7, 13, 16, 18, 19, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black, as cited in the previous Office Action, in view of Huennekens et al. (US 2003/0004866).

Re claim 1, Black teaches a biometric sensor to detect a proffered biometric sample and a device configured to associate the proffered biometric sample with user information and smartcard information to create a data packet. (FIG. 1A, 1C, abstract, 5A, 10A-11B, 14A-14B, paragraph [0090]+, and paragraph [0014]+). The Examiner has interpreted the information and biometric to constitute a data packet. As Black teaches the information can be stored remotely or locally, the examiner notes it would have been obvious to store the information in a database, since a database is well known and conventional in the art to conveniently storing and organizing data for easy access. As the information (data packet) is part of the authentication/registration process, it would obviously communicate with the system as part of the process.

Black is silent to the device associating the sample with a preset transaction limitation.

The Examiner notes that it is well known and conventional that credit cards have associated transaction limitations with them, for protection (security). Specifically, Huennekens et al. teaches that a credit limit is associated with a credit card account and that during a purchase the credit limit is verified (paragraph [0005]+).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of black with those of Huennekens.

One would have been motivated to do this for security; to have credit limit on purchasing power. The Examiner notes that as part of the registration process, information is associated with the proffered sample. The Examiner notes that it would have been obvious to one of ordinary skill in the art that the device associate the transaction limitation with the sample, as part of the process, in order to link not only the sample to information but also to a transaction

limitation for security. A device such as a controller/microprocessor/other equivalent electronic device would be an obvious expedient for such associating and is conventional in the art.

Re claim 2, the Examiner notes that Black teaches that the biometric is stored either on the smartcard/transponder or remotely. Accordingly, it would have been obvious to store, process, and verify the sample as part of the process to associate and authenticate/verify the sample, as is conventional in the art. Though silent to verification, the Examiner notes that it is obvious to verify a received sample in order to confirm that a complete and accurate sample was received, before storing, so that only a legitimate/complete sample is recorded (see FIG. 5A which teaches making sure that sample is acceptable, which can be interpreted as a verification). Additional conventional types of verification include verifying that the sample is real.

Re claim 4, association has been discussed above. The Examiner notes that it would have been obvious that different samples (different people) have different account information, thus providing uniqueness and security for distinct users.

Re claim 5, it has been discussed above that the data packet can be stored on a database. The Examiner notes that Black teaches that the stored information includes at least one of a sample, user information, terrorist information, and criminal information (FIG. 10A+ and FIG. 14A+ which teach user records). The storing of such information on a database is an obvious expedient to facilitate organizing and efficient data storage.

Re claim 6, it has been discussed above that the data packet can be stored locally or remotely. Accordingly, it would have been obvious to one of ordinary skill in the art that remote/local storing would include one of a remote server, merchant server, transponder-reader

system, transponder reader, sensor, and transponder itself. One would have been motivated to store it accordingly, based on desired security concerns.

Re claim 7, when stored remotely for example, the Examiner notes it would have been obvious that the database be operated by an authorized sample receiver, in order to ensure security.

Re claim 13, it has been discussed above that a fingerprint sample is obtained. It would have been obvious that a fingerprint be scanned, in order to obtain the fingerprint data to facilitate authentication/registration.

Re claim 16, it has been discussed above that accounts are associated with a transaction limitation (such as credit cards) for protection.

Re claim 18, a transaction limitation such as maximum transaction amount is conventional in the art for financial protection of the user, and is an obvious expedient.

Re claim 19, Black teaches (FIG. 1A) that the host computer can store the reference data. The Examiner has interpreted the host computer as biometric information registered with at least one of a third party biometric security vendor and government agency. The Examiner notes that as the transaction can take place remotely, it would have been obvious to one of ordinary skill in the art that the host computer can be such a party as claimed (for example the card/fob company the user is registered with) as a means for securely providing the biometric information to facilitate a transaction at a point of sale terminal. The claims do not recite what constitutes a third party biometric security vendor, let alone a first or second party vendor. Therefore, the Examiner believes that such an interpretation that the card/fob company themselves stores the registered samples, is a valid interpretation. Again, if a biometric is provided at a remote

terminal for a transaction, it would have been obvious that the sample be registered with that vendor to process the transaction (the sample must be accepted). With respect to government agencies, such registering is obviated by keeping track of illegal immigrants, criminals, etc.

Re claim 21, the limitations have been discussed above re claim 18.

5. Claims 8-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Huennekens et al., as discussed above, in view of Moebs et al. (US 2005/0065872).

The teachings of Black/Huennekens et al. have been discussed above.

Re claim 8, Black/Huennekens et al. are silent to primary and secondary associating of a biometric as claimed.

Moebs et al. teaches such limitations (paragraph [0017]).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black/Huennekens et al. with those of Moebs et al.

One would have been motivated to do this in order to provide for financial protection, for example.

Re claims 9-11 it has been discussed above that numerous people would use the system. It would have been obvious to one of ordinary skill in the art to associate different samples with different information in instances where there are multiple users of the system, for unique identification.

As such associating takes place electronically, it would have been obvious for the device to complete the associating, and as such devices are conventional and predictable for electronic processing.

6. Claims 12 and 15-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Huennekens et al., as discussed above, in view of de Sylva.

The teachings of Black/Huennekens et al. have been discussed above.

Re claim 12, Black teaches the device configured to verify is configured to facilitate the use of at least one secondary security procedure (signature, metrics FIG. 1C). Black teaches the use of a transaction record (paragraph [0125]) but is silent to the record occurring during unauthorized access attempts. However, the Examiner notes it would have been obvious to one of ordinary skill in the art to store such attempts in order to obtain security information regarding usage and attempts to access accounts illegally. Additionally, the Examiner notes that upon trying to use a card in excess of its credit limit (breaking a rule) that notification would obviously be provided to stop the transaction.

Black/Huennekens et al. is silent to the verification device sending a signal to the host device to notify that an established rule for the transponder is being violated.

De Sylva teaches remote database 32 stores non-authenticated data from the verifier (50) (paragraph [0032]).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black/Huennekens et al. with those of de Sylva.

One would have been motivated to do this in order to alert instances of fraud. It would have been obvious for the verification device to complete such steps, as it is responsible for verifying the sample, if the sample is not verified it would be obvious to create notification for fraud

Re claim 15, Black teaches that a unique identifier/customer number is associated with the user (FIG. 10A+). This is broadly interpreted as a personal identification number, or a unique means to verify a user/device. Additionally, the Examiner notes PIN-biometric combinations are well known and conventional in the art for increased security in systems. Therefore, using a PIN in addition to a biometric is an obvious expedient to increase security. The Examiner also notes that de Sylva teaches that prior art systems use biometric and PINs for access (paragraph [0013]), for security. It is obvious that the device that associates would perform such steps, as they are integral to the process of registering and storing data.

Re claim 16, de Sylva et al. teaches that a user can specify that transactions greater than a certain amount be charged to certain accounts while smaller purchases are charged to a different account (paragraph [0047]). Therefore it would have been obvious to have a preset amount for an account to control charges.

Re claim 17, the Examiner notes de Sylva teaches selection of an account can be made from a plurality of accounts, by using the record (30). Accordingly, it would have been obvious to have a device facilitate selection of the account, in accordance with the rules, in order for charges to automatically be made to comply with the rules (processor, controller, etc).

Response to Arguments

7. The Examiner notes Haala et al. (US 2005/0102524) teaches government being involved in the process to authenticate users and locate criminals, for example.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel I. Walsh whose telephone number is (571) 272-2409. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee can be reached on (571) 272-2398. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Daniel I Walsh
Examiner
Art Unit 2876
4-11-06

